UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

L.C. and N.C., individually and on behalf of all others similarly situated, by their parent and guardian, KEREN GELFAND, along with KEREN GELFAND, on behalf of herself and also on behalf of all others similarly situated, Plaintiffs, v. ANN & ROBERT H. LURIE CHILDREN'S HOSPITAL OF CHICAGO, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs L.C. and N.C., individually and on behalf of all others similarly situated, by their parent and guardian, KEREN GELFAND, along with KEREN GELFAND, on behalf of herself and also on behalf of all others similarly situated ("Plaintiffs"), brings this action against Defendant ANN & ROBERT H. LURIE CHILDREN'S HOSPITAL OF CHICAGO ("Defendant" or "Lurie Children's") and allege as follows based on personal knowledge as to their own acts and on investigation conducted by counsel as to all other allegations:

NATURE OF THE ACTION

1. Lurie Children's is a top-ranked children's hospital and healthcare provider in Illinois, and is "the largest pediatric provider in the region with a 140-year legacy of excellence."[1]

2. In providing medical care to children and families from across the country, Lurie Children's collects a significant amount of data - including patients' personal identifiable information ("PII") name, address, date of birth, dates of service, driver's license, email address,

[1] https://www.luriechildrens.org/en/who-we-are/ (last accessed July 10, 2024).

telephone number, Social Security number, as well as health information including health claims information, health plan, health plan beneficiary number, medical condition or diagnosis, medical record number, medical treatment, and prescription information[2] (the "PHI" or, collectively, the "Private Information. Lurie Children's collects, uses, and derives a benefit from its patients' extremely sensitive Private Information —and it assumes a significant duty to protect that information.

3. This class action arises out of a recent cyberattack and data breach (the "Data Breach") resulting from Lurie Children's failure to implement reasonable and industry-standard data security practices to protect its patients' personal identifying information, including Private Information.

4. Defendant disclosed on or about June 27, 2024 that the PII of over 792,000 current or former patients, including mostly children, has been compromised as a result of cyberattacks that occurred between January 26, 2024 and January 31, 2024.[3]

5. According to Lurie Children's Notice of Data Breach (the "Notice"), Lurie Children took certain systems offline on January 31, 2024 to protect their systems and their ability to continue operations.[4]

6. The Data Breach compromised and exposed patient's Private Information such as name, address, date of birth, dates of service, driver's license number, email address, health claims information, health plan, health plan beneficiary number, medical condition or diagnosis, medical

[2] https://www.luriechildrens.org/en/privacy-legal-information/notice-of-privacy-practices/ (last accessed July 10, 2024).
[3] https://www.luriechildrens.org/en/lurie-childrens-notifies-individuals-of-data-breach/ (last accessed July 10, 2024)
[4] *Id.*

record number, medical treatment, prescription information, Social Security number, and telephone number.[5]

7. This Data Breach was a ransomware attack which is a type of cybersecurity attack where the criminal deploys "ransomware" on a victim's computer system or data storage network until an untraceable cryptocurrency ransom is paid. Lurie Children's admits on its website that it "did not pay a ransom" but does not state that it was the victim of a ransomware attack.[6]

8. Rhysida, a ransomware group, claims to have been responsible for the Data Breach, and further claims to have sold it for approximately 60 bitcoins, or about $3.4 million.[7]

9. Lurie Children inexplicably waited nearly five months until June 27, 2024 to inform its patients that their PII and PHI could be compromised as a result of the Data Breach.[8] In cases dealing with data breaches, every moment is precious in order to recover data and take the necessary precautions to insulate from the countless harms caused by data breaches.

10. Lurie Children failed to protect Plaintiffs' and Class Members' PII/PHI therefore, Plaintiffs and Class Members have been exposed to actual harm consistent with the litany of injuries that data breaches cause, including (a) loss of value of PII, (b) loss of time spent dealing with the Data Breach, (c) imminent threat of and actual theft of PII by cybercriminals (d) financial loss, such as purchasing protective measures including credit monitoring, credit freezes, credit reports, and other means of detecting and mitigating identity theft and (e) any other types of quantifiable harm that stem from the breach, including out-of-pocket losses.

---

[5] *Id.*

[6] *Id.*

[7] https://www.beckershospitalreview.com/cybersecurity/hackers-say-they-sold-lurie-childrens-hospital-data-for-3-4m.html (last accessed July 10, 2024).

[8] *See* Template Notice sent to patients, available at https://www.mass.gov/doc/assigned-data-breach-number-2024-1211-ann-robert-h-lurie-childrens-hospital-of-chicago/download (last accessed July 10, 2024); *see also* Exs. A, B, and C (individualized notice letters with respect to L.C., N.C. and Keren Gelfand, respectively).

11. Plaintiffs, individually and on behalf of all others similarly situated, bring this Action, seeking to recover damages and non-monetary relief, as well as any other relief this Court may deem just and proper, as a result of Defendant's actions and/or nonactions that led and/or allowed the Data Breach to have occurred.

12. Defendant's offer to Plaintiffs and the putative Class of 24 months of "complimentary access to Experian IdentityWorks"[9] is wholly inadequate compared to what may affected victims may face for the rest of their lives due to the Data Breach.

PARTIES

13. Plaintiffs L.C. and N.C. are minors and, at all relevant times herein, have been residents and citizens of the State of Illinois. L.C. and N.C. bring this action by their parent and guardian, Keren Gelfand. The notice letters sent by Defendant with respect to Plaintiff L.C. and N.C. were addressed to their "Parent or Guardian", and advised that the recipient [Keren Gelfand] that "Your child or minor dependent has been identified as an individual whose information was impacted in this cybersecurity attack."[10]

14. Plaintiff Keren Gelfand is not a minor, and at all relevant times herein, has been a resident and citizen of the State of Illinois. The notice letters sent by Defendant with respect to Plaintiff Gelfand was addressed to her directly, and advised that "You have been identified as an individual whose information was impacted in this cybersecurity attack."[11]

15. Defendant Lurie Children's is an Illinois corporation with its principal place of business in Chicago, Illinois.

---

[9] https://www.mass.gov/doc/assigned-data-breach-number-2024-1211-ann-robert-h-lurie-childrens-hospital-of-chicago/download (last accessed July 10, 2024).

[10] *See* Exs. A & B.

[11] *See* Ex. C.

JURISDICTION AND VENUE

16. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are Class members who are diverse from Defendant, and (4) there are more than 100 Class members.

17. This Court has personal jurisdiction over Lurie Children's because Lurie Children's maintains its principal place of business in Chicago, Illinois.

18. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b)(1) because Defendant is a resident of this district.

FACTUAL ALLEGATIONS

I. Background

19. Defendant is based in Chicago, Illinois.

20. Defendant's patients, like Plaintiffs and Class members, provided certain PII and PHI to Defendant, which is necessary to obtain Defendant's services.[12]

21. In its business of providing medical services, Lurie Children's collects and stores' patients' personal information and medical information, including, at a minimum, names, addresses, Social Security numbers, health insurance information, and medical information.[13]

22. Lurie Children's also likely creates and maintains a considerable amount of PHI in the course of providing medical care and treatment. This PHI includes, but is not limited to, billing account numbers, financial information, medical record numbers, dates of service, provider names, and medical and clinical treatment information regarding care received from Lurie Children's.[14]

---

[12] https://www.luriechildrens.org/en/privacy-legal-information/notice-of-privacy-practices/ (last accessed July 10, 2024).
[13] *Id.*
[14] *Id.*

23. These records were and are stored on Lurie Children's networks. Defendant represented to patients and the public that they possess robust security features to protect Private Information and that they take their responsibility to protect Private Information seriously.

24. A copy of the Privacy Policy is maintained on Lurie Children's website, and states: "We are committed to protecting the privacy of children… Lurie Children's is committed to maintaining reasonable physical, technical, and administrative measures to protect your personal information."[15]

25. As a condition of receiving services from Defendant, Defendant requires that its patients entrust it with highly sensitive personal information.

26. Plaintiffs and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information.

II. The Data Breach

27. According to Defendant, between January 26, 2024 to January 31, 2024, Defendant learned that a vulnerability in their computer networks was exploited.

28. Defendant provided further information via its website:

> Ann & Robert H. Lurie Children's Hospital of Chicago ("Lurie Children's") has been investigating the nature and scope of a sophisticated cybersecurity attack that occurred earlier this year. Throughout our response to this matter, Lurie Children's has remained dedicated to the care and safety of our patients.
>
> Through Lurie Children's' ongoing investigation, we have determined that cybercriminals accessed Lurie Children's systems between January 26 and 31, 2024. On January 31, 2024, to protect our systems and our ability to continue operations, Lurie Children's took certain electronic systems offline, including our email, phones, and electronic health record system (Epic), and its patient portal (MyChart). Lurie Children's also activated our standard incident

[15] *Id.*

response procedures, including the Hospital Incident Command Structure (HICS). The Hospital implemented its downtime procedures, and we have remained open for patient care throughout the investigation. Additionally, we retained leading cybersecurity experts and legal counsel to work with our internal teams. We have worked closely with law enforcement as well.

Due to the complexity of the attack as well as our infrastructure, it has taken time to understand what happened and to identify the scope of impact to our systems and data. As part of our ongoing investigation, we thoroughly and methodically reviewed and analyzed impacted data contained on those systems. Through our investigation, Lurie Children's has determined that information relating to certain individuals, such as name, address, date of birth, dates of service, driver's license number, email address, health claims information, health plan, health plan beneficiary number, medical condition or diagnosis, medical record number, medical treatment, prescription information, Social Security number, and telephone number, was impacted. The information relating to a particular individual varies individual to individual. We have no indication that the cybercriminals accessed data stored in our electronic health record system (Epic), although certain information stored in other Lurie Children's systems was impacted.

At Lurie Children's, we take seriously the privacy of our patients' and team members' sensitive information. Lurie Children's did not pay a ransom. Experts have advised that making a payment to cybercriminals does not guarantee the deletion or retrieval of data that has been taken. Once our investigation team identified an amount of data that was impacted by the cybercriminals, we worked closely with law enforcement to retrieve that data.

Lurie Children's is in the process of notifying individuals whose data was impacted, including through mailing notification letters and other methods. Our notification material will identify resources to help protect their identity. Additionally, Lurie Children's is offering individuals whose data was impacted complimentary access to Experian IdentityWorks℠ for 24 months to help protect their information. Lurie Children's serves patients and patient families around the world, and individuals who live outside of the United States may receive those services if they're available in their country.

It is always a good practice to remain vigilant and to carefully review your online accounts, financial statements, and Explanations of Benefits from your health insurers for any unauthorized activity.

> Contact the company that maintains the account immediately if you detect any suspicious transactions or other activity you do not recognize.
>
> Lurie Children's has established an external toll-free call center to address the community's questions about notification, the cybersecurity attack and our response. If you have additional questions about the notification, any notification letter you may have received, or whether your information was impacted, you can contact the call center at 888-401-0575, Monday-Friday between 8 am and 8 pm, U.S. central time.
>
> We deeply regret that this cybersecurity attack occurred. Hospitals and health systems across the country face constantly evolving cybersecurity threats. For our part, we are working closely with our internal and external experts to further enhance the security of our systems.
>
> We remain incredibly grateful for the support and patience of our patients, patient-families, team members, community partners, research partners and broader Lurie Children's community throughout this matter. We look forward to continuing our longstanding mission of creating a healthier future for every child.[16]

29. The Data Breach compromised customers' personal information such as name, address, date of birth, dates of service, driver's license number, email address, health claims information, health plan, health plan beneficiary number, medical condition or diagnosis, medical record number, medical treatment, prescription information, Social Security number, and telephone number.[17]

30. The Data Breach affected almost 792,000 patients, including Plaintiffs and Class members, who entrusted their Private Information to Defendant.[18]

---

[16] https://www.luriechildrens.org/en/lurie-childrens-notifies-individuals-of-data-breach/ (last accessed July 10, 2024).

[17] *Id.*

[18] https://www.healthcarefacilitiestoday.com/posts/Update-on-Lurie-Childrens-Hospital-Cyberattack--29595 (last visited July 10, 2024).

31. Defendant sent a breach notification letter to affected customers on or around June 27, 2024. Lurie Children's waited nearly five months to inform its patients that their Private Information had been compromised as a result of the Data Breach.[19]

32. Defendant did not state why they waited nearly five months after the Data Breach before notifying affected patients.

33. Defendant did not state why it was unable to prevent the Data Breach or which security feature(s) failed. Additionally, Defendant did not state 1) how the unauthorized actors gained access 2) how Defendant failed to detect these intrusions, and 3) how Defendant intends to avoid these types of incidents in the future.

34. Defendant failed to prevent the Data Breach because it did not adhere to commonly accepted security standards and failed to detect that their databases were subject to a security breach.

III. Plaintiffs' Experience

35. Plaintiffs are very careful about sharing their sensitive Private Information and diligently maintain their Private Information in a safe and secure manner. Plaintiffs have never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

36. As a result of the Data Breach, Plaintiffs have and will continue to spend time trying to mitigate the consequences of the Data Breach. This includes time spent verifying the legitimacy of communications related to the Data Breach, and self-monitoring their accounts and credit reports to ensure no fraudulent activity has occurred.

[19] *See* Exs. A, B & C.

37. Plaintiffs suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and have anxiety and increased concerns for the loss of their privacy.

38. This time has been lost forever and cannot be recaptured. The harm caused to Plaintiffs cannot be undone.

39. Plaintiffs further suffered actual injury in the form of damages to and diminution in the value of their Private Information—a form of intangible property that Plaintiffs entrusted to Defendant, which was compromised in and as a result of the Data Breach.

40. Plaintiffs have suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from their Private Information being placed in the hands of cybercriminals.

41. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

42. Plaintiffs have a continuing interest in ensuring that their Private Information, which, upon information and belief, remains in Defendant's control, is protected, and safeguarded from future breaches.

IV. Injuries to Plaintiffs and Class members

43. As a direct and proximate result of Defendant's actions and omissions in failing to protect Plaintiffs and Class members' Private Information, Plaintiffs and Class members have been injured.

44. Plaintiffs and Class members have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages, including spending substantial amounts of time monitoring accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud.

45. In addition to the irreparable damage that may result from the theft of Private Information, identity theft victims must spend numerous hours and their own money repairing the impacts caused by a breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[20]

46. In addition to fraudulent charges and damage to their credit, Plaintiffs and Class members may spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

47. Additionally, Plaintiffs and Class members have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their Private Information is used, the diminution in the value or use of their Private Information, and the loss of privacy.

V. Lurie Children's has a duty to protect patients' personal information

48. As a pediatric hospital, Lurie Children's knew or should have known that protecting its patients' PII/PHI was of the utmost importance.

49. Defendant could have prevented this Data Breach by properly securing and encrypting the Private Information of Plaintiffs and Class members. Alternatively, Defendant

[20] U.S. Dep't of Justice, *Victims of Identity Theft, 2014* (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

could have destroyed the data they no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

50. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

51. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class members from being compromised.

52. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[21] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[22]

53. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class members are long lasting and severe. Once Private Information is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

[21] 17 C.F.R. § 248.201 (2013).
[22] *Id*.

VI. The Value of Private Information

54. It is well known that Private Information is an invaluable commodity and a frequent target of hackers.

55. People place a high value not only on their Private Information, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[23]

56. People are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[24] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiffs and Class members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all problems . . . and won't guarantee . . . a fresh start."[25]

57. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[26] Experian reports

---

[23] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.

[24] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html.

[25] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf.

[26] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[27] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[28]

58. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[29]

59. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse.[30] In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

[27] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[28] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

[29] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf.

[30] AARP, *Is it possible to get a new Social Security number?,* https://www.aarp.org/retirement/social-security/questions-answers/new-number.html

60. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[31]

61. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

62. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[32]

63. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

64. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.

[31] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

[32] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

> As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[33]

65. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class members, including Social Security numbers, and of the foreseeable consequences that would occur if their data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class members as a result of a breach.

66. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.[34] Plaintiffs and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

67. Defendant knew of the unique type and the significant volume of data contained in the Private Information that Defendant stored on their networks, and, thus, the significant number of individuals who would be harmed by the exposure of the data.

68. The injuries to Plaintiffs and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class members.

VII. Industry Standards for Data Security

69. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[35]

---

[33] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.
[34] *Id.*
[35] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

70. In light of the numerous high-profile data breaches targeting companies like Yahoo, Facebook, and LinkedIn, Defendant knew of the importance of safeguarding Private Information, as well as of the foreseeable consequences of its systems being breached.[36]

71. Therefore, the increase in such attacks, and the attendant risk of future attacks, were widely known to the public and to anyone in Defendant's industry, including Defendant.

72. Security standards commonly accepted among businesses that store Private Information using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for Private Information;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

73. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[37] and protection of Private Information[38] which includes basic security standards applicable to all types of businesses.

---

[36] Michael Hill and Dan Swinhoe, *The 15 biggest data breaches of the 21st century*, https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html

[37] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[38] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

74. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as

an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[39]

76. Because Plaintiffs and Class members entrusted Defendant with Private Information, Defendant had a duty to keep the Private Information secure.

77. Plaintiffs and Class members reasonably expect that when their Private Information is provided to a sophisticated business for a specific purpose, that business will safeguard their Private Information and use it only for that purpose.

78. Nonetheless, Defendant failed to prevent the Data Breach. Had Defendant properly maintained and adequately protected their systems, they could have prevented the Data Breach.

VIII. HIPAA Standards and Violations

79. In addition to failing to follow universal data security practices, Defendant failed to follow healthcare industry standard security practices, including:

a. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. 164.306(a)(2);

b. Failing to ensure compliance with HIPAA security standards by their workforce or agents in violation of 45 C.F.R 164.306(a)(94);

c. Failing to effectively train all members of its workforce and its agents on the policies and procedures with respect to PHI as necessary to maintain the security of PHI in violation of C.F.R. 164.530(b) and 45 C.F.R. 164.308(a)(5); and

d. Failing to design and implement and enforce policies and procedures to establish administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. 164.530(c).

[39] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

80. Lurie Children's is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[40] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

81. HIPAA's Security Rule requires Lurie Children's to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

82. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Lurie Children's to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[41]

CLASS ALLEGATIONS

83. This action is brought as a class action pursuant to Fed. R. Civ. P. 23.

84. The Class is defined as follows:

> **Nationwide Class:** All persons whose Private Information was maintained on Defendant's servers that were compromised in the Data Breach.

85. The Class excludes the following: Defendant, their affiliates, and their current and former employees, officers and directors, and the Judge assigned to this case.

[40] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.
[41] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

86. The Class definition may be modified, changed, or expanded based upon discovery and further investigation.

87. *Numerosity*: The Class is so numerous that joinder of all members is impracticable, evidenced by the large number of individuals presently known to have been injured by Defendant's conduct. The Class is ascertainable by records in the possession of Defendant or third parties.

88. *Commonality*: Questions of law or fact common to the Class include, without limitation:

a. Whether Defendant owed a duty or duties to Plaintiffs and Class members to exercise due care in collecting, storing, safeguarding, and obtaining their Private Information;

b. Whether Defendant breached that duty or those duties;

c. Whether Defendant failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

d. Whether the security provided by Defendant was satisfactory to protect Private Information as compared to industry standards;

e. Whether Defendant misrepresented or failed to provide adequate information regarding the type of security practices used;

f. Whether Defendant knew or should have known that they did not employ reasonable measures to keep Plaintiffs and Class members' Private Information secure and prevent loss or misuse of that Private Information;

g. Whether Defendant acted negligently in connection with the monitoring and protecting of Plaintiffs and Class members' Private Information;

h. Whether Defendant's conduct was intentional, willful, or negligent;

i. Whether Plaintiffs and Class members suffered damages as a result of Defendant's conduct, omissions, or misrepresentations; and

j. Whether Plaintiffs and Class members are entitled to injunctive, declarative, and monetary relief as a result of Defendant's conduct.

89. *Typicality*: Plaintiffs' claims are typical of the claims of Class members. Plaintiffs and Class members were injured and suffered damages in substantially the same manner, have the same claims against Defendant relating to the same course of conduct, and are entitled to relief under the same legal theories.

90. *Adequacy*: Plaintiffs will fairly and adequately protect the interests of the Class and have no interests antagonistic to those of the Class. Plaintiffs' counsel are experienced in the prosecution of complex class actions, including actions with issues, claims, and defenses similar to the present case.

91. *Predominance and superiority*: Questions of law or fact common to Class members predominate over any questions affecting individual members. A class action is superior to other available methods for the fair and efficient adjudication of this case because individual joinder of all Class members is impracticable and the amount at issue for each Class member would not justify the cost of litigating individual claims. Should individual Class members be required to bring separate actions, this Court would be confronted with a multiplicity of lawsuits burdening the court system while also creating the risk of inconsistent rulings and contradictory judgments. In contrast to proceeding on a case-by-case basis, in which inconsistent results will magnify the delay and expense to all parties and the court system, this class action presents far fewer management difficulties while providing unitary adjudication, economies of scale and comprehensive supervision by a single court. There are no known difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

92. Accordingly, this class action may be maintained pursuant to Fed. R. Civ. P. 23(b)(3).

93. Defendant's unlawful conduct applies generally to all Class members, thereby making appropriate final equitable relief with respect to the Class as a whole.

94. Accordingly, this class action may be maintained pursuant to Fed. R. Civ. P. 23(b)(2).

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

95. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

96. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services, which solicitations and services affect commerce.

97. Plaintiffs and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

98. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

99. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their servers—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

100. Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

101. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

102. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. However, despite learning of the breach no later than January 31, 2024, Defendant did not notice affected victims until June 27, 2024 – a delay of nearly five months.

103. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

104. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of being patients of Defendant.

105. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

106. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

107. Defendant also had a duty to exercise appropriate practices to remove former patients' Private Information once it was no longer required to retain pursuant to regulations.

108. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

109. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to periodically ensure that its email system had reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to remove former patients' and employees' Private Information it was no longer required to retain pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

110. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

111. Plaintiffs and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

112. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

113. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

114. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

115. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

116. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

117. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

118. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

119. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

120. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

121. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

122. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the

actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

123. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

124. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

125. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

126. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's

possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

127. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

128. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

129. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

130. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

131. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class)

132. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

133. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

134. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

135. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. However, despite learning of the breach no later than January 31, 2024, Defendant did not notice affected victims until June 27, 2024 – a delay of nearly five months.

136. Defendant violated Section 5 of the FTC Act, HIPAA, and similar state statutes by failing to use reasonable measures to protect Private Information and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

137. Defendant's violation of Section 5 of the FTC Act, HIPAA, and similar state statutes constitutes negligence *per se*.

138. Class Members are consumers within the class of persons Section 5 of the FTC Act, HIPAA, and similar state statutes were intended to protect.

139. Moreover, the harm that has occurred is the type of harm the FTC Act, HIPAA, and similar state statutes were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

140. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

141. Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

142. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

143. Plaintiffs and the Class entrusted their Private Information to Defendant. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant

agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

144. In its Notice of Privacy Practices, Defendant represented the limited circumstances for which it may disclose Plaintiffs' and Class Members' Private Information to authorized third parties, wholly implying unauthorized third parties would not be privy to this Private Information and that Defendant would take necessary measures to protect against such unauthorized access.[42]

145. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

146. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered into protect such information and to destroy any Private Information that it was no longer required to maintain.

147. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing.

148. Defendant solicited, offered, and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices.

149. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

150. In accepting the Private Information of Plaintiffs and Class Members, Defendant understood and agreed that they were required to reasonably safeguard the Private Information from unauthorized access or disclosure.

[42] https://www.luriechildrens.org/en/privacy-legal-information/notice-of-privacy-practices/ (last visited July 10, 2024).

151. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, the FTC Act, and were consistent with industry standards.

152. As a result of services contracted by Plaintiffs and Class Members, Defendant earned money with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

153. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

154. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

155. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

156. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their Private Information or to destroy it once it was no longer necessary to retain the Private Information.

157. As a direct and proximate result of Defendant's breach of the implied promises, Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Plaintiffs and Class Members sustained incidental and consequential damages including: (a) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) financial "out of pocket" costs incurred due to actual identity theft; (d)

spam and targeted marketing emails; (f) diminution of value of their Private Information; (g) future costs of identity theft monitoring; (h) and the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

158. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach to be determined at trial.

159. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
[In the Alternative]
(On Behalf of Plaintiffs and the Class)

160. Plaintiffs repeat, re-allege, and incorporate by reference, all other paragraphs of this complaint.

161. Plaintiffs bring this claim in the alternative to their breach of implied contract claim.

162. Plaintiffs and Class Members conferred a benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have had their Private Information protected with adequate data security.

163. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form of their Private Information. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

164. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and some Class Members.

165. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

166. Defendant, however, failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

167. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

168. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

169. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

170. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own

profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

171. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

172. Plaintiffs and Class Members have no adequate remedy at law.

173. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

174. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

175. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them.

In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services

176. Accordingly, Plaintiffs and Class members respectfully request that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of their wrongful conduct, including specifically, the amounts that Defendant should have spent to provide reasonable and adequate data security to protect Plaintiffs and Class members' Private Information, and compensatory damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays for a judgment as follows:

a. For an order certifying the Class, appointing Plaintiffs as Class Representative, and appointing the law firms representing Plaintiffs as counsel for the Class;

b. For compensatory, punitive, statutory, and treble damages in an amount to be determined at trial;

c. Payment of costs and expenses of suit herein incurred;

d. Both pre-and post-judgment interest on any amounts awarded;

e. Payment of reasonable attorneys' fees and expert fees;

f. Such other and further relief as the Court may deem proper.

JURY DEMAND

Plaintiffs, individually, and on behalf of the Plaintiffs' Class, hereby demand a trial by jury for all issues triable by jury.

Dated: July 11, 2024

Respectfully submitted,

/s/ Gary M. Klinger
Gary M. Klinger
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (866) 252-0878
gklinger@milberg.com

Charles E. Schaffer*
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: (215) 592-1500
cschaffer@lfsblaw.com

Jeffrey S. Goldenberg *
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Tel: (513) 345-8291
jgoldenberg@gs-legal.com

Brett R. Cohen*
LEEDS BROWN LAW, P.C.
One Old Country Road, Suite 347
Carle Place, NY 11514
Tel: (516) 873-9550
bcohen@leedsbrownlaw.com

Counsel for Plaintiffs and Proposed Class

* *Pro Hac Vice* forthcoming